CLAIMS:

1. A method of distributing certificates to mobile devices by establishing a mobile ad hock network (MANET) between a plurality of mobile devices at a predetermined time and distributing a certificate through said mobile ad hoc network to a respective one of said mobile devices.
2. The method of claim 1 wherein the times for which a certificate is valid is correlated to the said predetermined time for establishing said MANET.
3. The method of claim 1 wherein a device that is unable to retrieve its certificate within a preset time after the establishment of a MANET subsequently attempts to participate in ad-hoc networks prior to the next predetermined time to retrieve its certificate.
4. The method of claim 1 wherein a device that is unable to retrieve its certificate within an amount of time after the MANET establishment initiates a cellular packet data call to fetch its certificate.
5. The method of claim 1 wherein an entity tracks which mobile devices have received currently valid certificates.
6. The method of claim 5 wherein a certificate of a device which has not received an up-to-date certificate is distributed to another device that communicates with said entity.
7. The method of claim 1 wherein the predetermined time for establishing the MANET is determined dynamically based upon measurements of times at which mobile devices encounter each other.
8. The method of claim 1 wherein the information in said distributed certificate comprises a subset of the full certificate information and the subset includes changed timing information and a signature.
9. A method of distributing certificates in a mobile ad-hoc network having an access point to provide a connection to a communication network and a plurality of mobile devices to be connected to said communication network through said access point, said method comprising the steps of retrieving and storing at said access point certificates associated with respective ones of said devices and forwarding said certificates through said mobile ad-hoc network to said respective device.
10. The method of claim 9 wherein said access point queries devices with which it can exchange packets to determine their embedded root key.

11. The method of claim 10 wherein the access point fetches certificates based upon said embedded root keys.

12. A method of distributing certificates within a mobile ad-hoc network wherein an online entity associated with a device is responsible for both distributing the device's certificate and for fetching other certificates needed to allow validation by another device in said network.

13. The method of claim 12 wherein said device is responsible for collecting embedded root keys of other devices with which it comes in contact with.

14. The method of claim 13 wherein said root keys are reported to the online entity.

15. The method of claim 14 wherein said online entity returns other certificates to the device based upon the reported root keys.

16. A method of securely setting a time source in a first device from a second device comprising the steps of: establishing a shared secret between the two devices using certificates; storing the shared secret in a non-volatile memory; a first of said devices authenticating a second of said devices using the shared secret; and transferring the time from the second device to the first device.

17. The method of claim 16 wherein the shared secret is destroyed after an expiration time.

18. The method of claim 16 wherein the first device subsequently sets its clock via a secure time source when it subsequently can establish a connection thereto.

19. A method of validating wherein a certificate presented to a first device by a second device is used for the validation if the second device's certificate has not expired and wherein the first device uses for the validation a certificate fetched based upon a pointer presented by the second device if the second device's certificate has expired.

20. A method of distributing certificates wherein a first device cannot retrieve a certificate at a first time because there is no connectivity to the internet comprising the steps of: requesting assistance of other devices if the certificate has still not been received by a second time; having a second device of the other devices request the certificate on behalf of the first device when the second device has connectivity to the internet; having the second device reestablish communication with the first device; and sending the certificate from the second device to the first device.